REMARKS

This Amendment responds to the Office Action dated February 25, 2002 in which the Examiner rejected claims 1-20 under 35 U.S.C. § 103.

Applicants would like to thank the Examiner for the telephone interview on July 18, 2002 in which the Examiner said that our arguments appear to be valid and will be considered when the Amendment is filed.

As indicated above, the specification has been amended in order to correct minor informalities. It is respectfully requested that the Examiner approves the corrections.

Claim 1 claims a vehicle-mounted communication device comprising a transmitting/ receiving means and a relay means. The transmitting/receiving means is provided for communication of information with a road-side communication means located at a road side. The relay means is for relaying encryption information received from the road side by the transmitting/ receiving means to an IC card. The IC card includes storage means for storing user information regarding a balance of charges and also includes encryption means that encrypts and outputs output information based on the user information and decodes encrypted input information regarding the user information.

Through the structure of the claimed invention having a relay means for relaying encrypted information received from the road side to an IC card, as claimed in claim 1, the claimed invention provides a vehicle-mounted communication device that can improve security. The prior art does not show, teach or suggest the invention as claimed in claim 1.

Claim 8 claims a road-to-vehicle communication device comprising a road-side control means, an information control means and a vehicle-mounted control means. The road-side control means is located at a road side, and includes a road-side communication means provided for intercommunication of information with a vehicle-mounted communication means. The road-side control means also includes a first encryption means for encrypting transmitted information and decoding received information, with a first electronic key. The information control means includes an information transfer means which stores therein user information regarding at least one of a vehicle and a user and through which information is mutually transferred with respect to the vehicle-mounted communication means. The information control means also includes a second encryption means for encrypting output information and decoding input information, with a second electronic key. The vehicle-mounted control means is installed on a vehicle side, and includes the vehicle-mounted communication means provided for intercommunication of information with respect to the road-side communication device and for mutual transfer of information with respect to the information control means. The vehicle-mounted control means also includes a third encryption means which, during the communication of information, encrypts transmitted information and decodes received information with the first electronic key, and which during the transfer of information, encrypts output information and decodes input information with the second electronic key.

Through the structure of the claimed invention having a road-side control means including a first encryption means with a first electronic key, an information control means including a second encryption means with a second electronic key and a vehicle-mounted

control means with a third encryption means which uses the first electronic key during communication of information and which uses the second electronic key during transfer of information, as claimed in claim 8, the claimed invention provides a road-to-vehicle communication device in which the disclosure of the secrecy of a system can be kept to a minimum even when the disclosure of one electronic key becomes known. The prior art does not show, teach or suggest the invention as claimed in claim 8.

Claims 1-7 and 10-20 were rejected under 35 U.S.C. §103 as being unpatentable over *Brockelsby et al* (U.S. Patent No. 5,631,642) in view of *Giniger et al* (U.S. Patent No. 6,199,043) and further in view of *Johnson, Jr.* (U.S. Patent No. 6,078,888).

Applicants respectfully traverse the Examiner's rejection of the claims under 35 U.S.C. §103. The claims have been reviewed in light of the Office Action, and for reasons which will be set forth below, it is respectfully requested that the Examiner withdraws the rejection to the claims and allows the claims to issue.

Brockelsby et al appears to disclose a mobile object tracking system, and in particular a vehicle tracking system. (col. 1, lines 5-9) Referring to FIG. 1, a vehicle tracking system 10 includes an array of signpost stations 12.1 to 12.14 generally positioned at nodes, or key intersection points in a road network 13. Each signpost station 12.1 to 12.14 has a respective area of coverage, of footprint 14.1 to 14.4 with a radius of approximately 50 m. (col. 3, lines 54-59) A protected vehicle 18 is fitted with a beacon unit 20 at a hidden location, the unit including a vehicle transmitter and a vehicle receiver. A remote actuator 19 carried on a key ring, for instance, allows the beacon unit 20 to be armed and disarmed externally of the vehicle. The beacon unit provides an indication that

it has been armed by flashing the vehicle's lights or a dashboard-based light, or alternatively by sounding the hooter or an audible buzzer mounted on the dashboard. When the beacon unit is armed, one or more sensors, such as a motion sensor or a door-mounted microswitch, will sense unauthorized entry into the vehicle and will cause the beacon unit to transmit intermittently a brief radio distress signal containing vehicle identification details, together with a signpost signal which is received from a proximate signpost station such as the signpost station 12.6 when the vehicle traverses the signpost footprint 14.6. (col. 4, lines 8-23) A receiver network comprises a plurality of fixed receiving stations 22.1 to 22.3 which are more sparsely arranged than the signposts, with an operating range of approximately 6 km. A combined signal 24 transmitted from the beacon unit 20 is received at the receiving station 22.2. This combined signal 24, which is modulated both with a beacon identification signal identifying the signpost station 12.6 and with a vehicle identification signal identifying the vehicle 18, is relayed from the receiving station 22.2 to a central control station 26 via a telephone or radio link 28. The other receiving stations 22.1 and 22.3 are similarly connected to the central control station 26. The receiving stations 22.1 to 22.3 are completely automatic in locating stolen vehicles and reporting the information to central control stations 26. (col. 4, lines 34-47)

Thus, *Brockelsby et al* merely discloses a vehicle tracking system 10 including signpost stations 12, a beacon unit 20 mounted on a vehicle 18, a receiver network comprising fixed stations 22 and a central control station 26. Nothing in *Brockelsby et al* shows, teaches or suggests a relay means for relaying encryption information from the road side to an IC card as claimed in claim 1. Rather, the beacon unit 20, which is mounted on

the vehicle 18, does not receive encrypted information from the signpost stations and does not relay the information to an IC card but rather relays it to a fixed receiver station 22.

Giniger et al appears to disclose that it may be desirable to dynamically provide a mobile user with information that is particularly related to the user's present location. (col. 1, lines 10-12) Communications between the mobile unit and the central site server are encrypted. Accordingly, the mobile unit's means for sending the present position information to the central site server comprises means for encrypting the present position information; and means, coupled to the encrypting means, for sending the encrypted present position information to the central site server. Furthermore, the mobile unit's means for receiving response information from the central site server comprises means for receiving encrypted response information from the central site server; and means, coupled to the encrypted response information receiving means, for decrypting the encrypted response information. The central site server's means for receiving the present position information from the mobile unit comprises means for receiving the encrypted present position information via the bidirectional communications link; and means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information. The central site server's means for sending the retrieved response information to the mobile unit comprises means for encrypting the retrieved response information; and means, coupled to the retrieved response information encrypting means, for sending the encrypted retrieved response information to the mobile unit via the bidirectional communications link. (col. 6, lines 19-43)

Thus, *Giniger et al* merely discloses communication between a mobile unit and a central site server. Nothing in *Giniger et al* shows, teaches or suggests a relay means for relaying information received from a road side to an IC card as claimed in claim 1. Rather, *Giniger et al* merely discloses communication between a mobile unit and a central site server.

Johnson, Jr. appears to disclose providing secure transactions between a local transaction device and a remote communication device and, more particularly, to a transponder fuel dispensing system for providing secure authorizations and transactions using the transponder in a fuel delivery, retail sales and service environment. (col. 1, lines 5-10) Secure transactions are provided with a tag and POS device associated with a host network authorization system. In doing so, the tag is adapted to bi-directionally communicate with a POS device, preferably a fuel dispenser, which further communicates with a host network to provide authorization of the tag and carry out any desired purchases or transactions. To avoid transmitting data from which valuable account or financial information could be derived between the tag and POS device or the POS device and the host network system, all or a majority of account and financial information requiring absolute security are only maintained at the host network. Neither the tag nor the POS device has or has access to critical financial or account information. But, the security system will also provide high levels of security for applications requiring transmission of such information. (col. 2, lines 61 through col. 3, line 9) Preferably, the tag is authenticated using identical cryptography techniques known only by the tag and host, but not by the POS device. Initially, the communication electronics of POS device, acting as

an interrogator, will continuously scan for a tag within the field. Once a tag comes within the field in response to the interrogator, the interrogator will recover the tag's identifier, hereinafter referred to as the ID number, from the tag. The POS device will generate authentication check data, preferably a random number, and send it to the tag for encryption. The tag then encrypts the random number with an encryption technique using a main cryptography key and transmits the encrypted random number back to the POS device. The interrogator passes the ID number, the encrypted random number and the original random number to the host through the associated POS device. The host determines or calculates the main cryptography key used in the tag from the tag ID number. The host encrypts the random number sent from the POS device and compares it with the encrypted random number sent from the tag through the POS device. The host then compares the encrypted random numbers encrypted by the host and the tag. If these numbers match, the host signals the POS device that the tag is valid. To further enhance security, the main cryptography key stored in the tag and determined or calculated by the host is only used for authentication of the tag. Data transfers or transactions between the tag and host through the POS device requiring security are encrypted and decrypted as necessary by the tag and host using a session key, which is different then the main cryptography key. Preferably, a new session key is generated for each transaction and is a function of a random number, independently generated in the tag and host, as well as the main encryption key. The tag random number is preferably generated upon receipt of the random number generated at the POS device. The tag random number is transmitted to the host through the POS device so that both the tag and host can independently generate the

session key capable of encrypting and decrypting data at either the host or the tag. The method used to generate the session key from the tag random number must be the same in both the host and tag. Similarly, the electronics in the tag and host are used to encrypt the random number generated at the POS device. (col. 3, lines 21-64) The secure transaction system 10 includes or is associated with three major subsystems: a remote communication unit 100 (hereinafter a tag); a POS device 200 and a host network 300. In general, remote communication units 100 are adapted to communicate with and through the POS device 200 in order to obtain authorization and communicate information to and from the host network 300. The tag 100 may also communicate with the POS device 200 or other local sources 32 directly. Various means of security are employed depending on the information being communicated and the source and destination of the information. Importantly, the tag 100 and host network 300 are adapted to encrypt and decrypt certain communications there-between, while the POS device 200 primarily only relays the encrypted information sent between the tag 100 and host network 300. Preferably to enhance security, the POS device 200 is unable to decrypt such information. (col. 5, lines 48-65)

Thus, *Johnson, Jr.* merely discloses a tag 100 which can be mounted in a vehicle 12. Thus, nothing in *Johnson, Jr.* shows, teaches or suggests a vehicle-mounted communication device comprising a relay means for relaying information received from the road side to an IC card as claimed in claim 1. Rather, the only vehicle-mounted device is tag 100 in *Johnson, Jr.*

Since nothing in *Brockelsby et al*, *Giniger et al* or *Johnson, Jr.* shows, teaches or suggests a vehicle-mounted communication device comprising a relay means for relaying

information received from the road side to an IC card as claimed in claim 1, it is respectfully requested that the Examiner withdraws the rejection to claim 1 under 35 U.S.C. §103.

Claims 2-7 and 10-20 depend from claim 1 and recite additional features. It is respectfully submitted that claims 2-7 and 10-20 are not unpatentable within the meaning of 35 U.S.C. §103 over *Brockelsby et al*, *Giniger et al* and *Johnson, Jr.* at least for the reasons as set forth above. Therefore, it is respectfully requested that the Examiner withdraws the rejection to claims 2-7 and 10-20 under 35 U.S.C. §103.

Claims 8-9 were rejected under 35 U.S.C. §103 as being unpatentable over *Brockelsby et al*, in view of *Giniger et al* and further in view of *Johnson, Jr.*

Applicants respectfully traverse the Examiner's rejection of claims 8-9 under 35 U.S.C. §103. The claims have been reviewed in light of the Office Action, and for reasons which will be set forth below, it is respectfully requested that the Examiner withdraws the rejection to the claims and allows the claims to issue.

As discussed above, *Brockelsby et al* merely discloses a vehicle tracking system 10 including signpost stations 12, a beacon unit 20 mounted in a vehicle 18, fixed receiver stations 22 and a central control station 26. Nothing in *Brockelsby et al* shows, teaches or suggests that any of these units include encryption means with encryption keys as claimed in claim 8. In particular, nothing in *Brockelsby et al* shows, teaches or suggests a road-side control means including a first encryption means with a first electronic key, an information control means including a second encryption means with a second electronic key and a vehicle-mounted control means including a third encryption means using the first electronic

key during communication of information and using the second electronic key during transfer of information as claimed in claim 8. Rather, nothing in *Brockelsby et al* shows, teaches or suggests encrypting information.

Giniger et al appears to disclose communication between a mobile unit and a central site server which send and receive encrypted information therebetween. Thus nothing in *Giniger et al* shows, teaches or suggests a road-side control means located at a road side and including first encryption means with a first electronic key as claimed in claim 8. Furthermore, nothing in *Giniger et al* shows, teaches or suggests an information control means through which information is mutually transferred and a vehicle-mounted control means for intercommunication of information with the road-side communication device and transfer of information to the information control means and including a third encryption means using a first electronic key during communication of information and using a second electronic key during transfer of information as claimed in claim 8. Rather, *Giniger et al* merely discloses a mobile unit and a central site server between which communications are encrypted.

Johnson, Jr. as discussed above merely discloses a) a main cryptographic key stored in the tag 100 and determined or calculated by the host 300 and used only for authentication of the tag and b) a sessions key which is used when data is transferred between the tag and host through the POS device 200. Thus, nothing in *Johnson, Jr.* shows, teaches or suggests a vehicle-mounted control means including an encryption means which uses a first electronic key during communication of information and uses a second electronic key

during transfer of information as claimed in claim 8. Rather, *Johnson, Jr.* merely discloses using a main cryptographic key for authentication and using a session key for data transfer.

Additionally, *Johnson, Jr.* discloses that the POS device 200 primarily only relays encrypted information between the tag 100 and network 300. Thus, nothing in *Johnson, Jr.* shows, teaches or suggests a road-side control means located at a road side including first encryption means having a first electronic key as claimed in claim 8. Rather, *Johnson, Jr.* teaches away from the claimed invention and merely discloses a device 200 which relays information.

Since nothing in *Brockelsby et al*, *Giniger et al* or *Johnson, Jr.* shows, teaches or suggests a) a road-to-vehicle communication device comprising the road-side control means with first encryption means having a first electronic key, b) information control means including a second encryption means with a second electronic key and c) a vehicle-mounted control means including a third encryption means using a first electronic key during communication of information and using a second electronic key during transfer of information as claimed in claim 8, it is respectfully requested that the Examiner withdraws the rejection to claim 8 under 35 U.S.C. §103.

Claim 9 depends from claim 8 and recites additional features. It is respectfully submitted that claim 9 would not have been obvious within the meaning of 35 U.S.C. §103 over *Brockelsby et al*, *Giniger et al* and *Johnson, Jr.* at least for the reasons as set forth above. Therefore, it is respectfully requested that the Examiner withdraws the rejection to claim 9 under 35 U.S.C. §103.

The prior art of record, which is not relied upon, is acknowledged. The references taken singularly or in combination do not anticipate or make obvious the claimed invention.

Thus it now appears that the application is in condition for reconsideration and allowance. Reconsideration and allowance at an early date are respectfully requested.

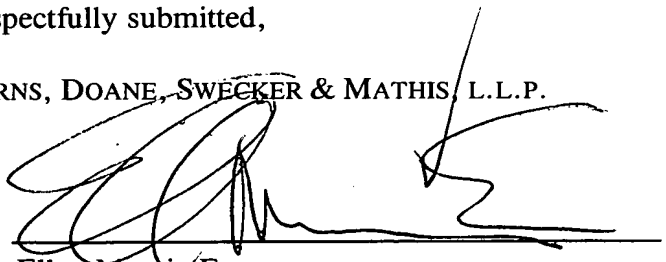
If for any reason the Examiner feels that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this case.

In the event that this paper is not timely filed within the currently set shortened statutory period, applicants respectfully petition for an appropriate extension of time. The fees for such extension of time may be charged to our Deposit Account No. 02-4800.

In the event that any additional fees are due with this paper, please charge our Deposit Account No. 02-4800.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: 

Ellen Marcie Emas
Registration No. 32,131

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: July 24, 2002

Mark-up of Specification

Paragraph beginning at page 8, line 9

At the vehicle-mounted communication device of the invention of claim 1 intercommunication of information is carried out with respect to the road-side communication means located at the road [said] side, with the transmitting/receiving means. The IC card is attachable and detachable at the vehicle-mounted communication device and stores in the storage means the user information regarding the balance of charges. The encryption means encrypts output information based on the user information and then outputs. The encryption means also decodes the encrypted input information regarding the user information. Among the information received from the road side by the transmitting/receiving means, the encryption information is relayed to the IC card by the relay means. Accordingly, the encryption information passes through the vehicle-mounted communication device in a form of being left unchanged, and thus, the secrecy of the encryption information is maintained and the security thereof is protected.